

## REMARKS

### **Explanation of Claim Amendments:**

Independent claims 1, 7, 10, and 14 have been amended to replace the term "some" that the Examiner found objectionable with the term "at least two," which is believed to be more definite. Claims 1, 2, 4, and 5 have been amended to address the rejection under 35 U.S.C. §112, second paragraph, as articulated by the Examiner in his comments to the Advisory Action mailed January 11, 2006. No matter has been entered and no new issues have been raised. Claims 8-9, 11-13, and 15-18 have not been amended. Claims 1-2, 4-5, and 7-18 remain in the application.

### **Section 112, Second Paragraph, Rejection**

In the Final Rejection, claims 1, 2, 4, 5, and 7-18 were rejected under 35 U.S.C. §112, second paragraph, as allegedly being indefinite. This rejection is respectfully traversed.

Independent claim 1 was rejected for alleged lack of clear antecedent for the limitation "the subset" in lines 13 and 14. Claim 2 was also rejected for use of "the subset" in line 2. Claims 1, 2, 4, and 5 have been amended to clarify to which "subset" the language refers. Withdrawal of the indefiniteness rejection of claims 1, 2, 4, and 5 is solicited.

Independent claims 1, 7, 10, and 14 were further rejected as indefinite for use of the term "some" to define the subsets. As noted above, independent claims 1, 7, 10, and 14 have been amended to replace the term "some" with the term "at least two," which is believed to be more definite. Withdrawal of the indefiniteness rejection of claims 1, 2, 4, 5, and 7-18 is solicited.

### **Section 103 Rejections:**

Claims 1, 2, 4, and 5 stand rejected under 35 U.S.C. §103(a) as allegedly being obvious over Matyas, Jr. et al. (US 6,697,947) in view of Schneier (*Applied Cryptography* article); claims 7-17 stand rejected under 35 U.S.C. §103(a) as allegedly being obvious over Matyas, Jr. et al. and Schneier in view of the portable fingerprint recognition and transmission device referenced in paragraph [0012] of the specification (admitted prior art); and claim 18 stands rejected under 35 U.S.C. §103(a) as allegedly being obvious over Matyas, Jr. et al., Schneier, and the admitted prior art in view of Schneider et al. (US 5,456,256). These rejections are respectfully traversed for the reasons given below.

As set forth in M.P.E.P. §§2142-2143.03, in order to establish a *prima facie* case of obviousness, patent examiners are required to establish three criteria: (1) there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings; (2) there must be a reasonable expectation of success; and (3) the prior art reference, or combination of references, must teach or suggest all the claim limitations. The examiner bears the initial burden of factually supporting any *prima facie* conclusion of obviousness. To make a proper obviousness determination, the examiner must “step backward in time and into the shoes worn by the hypothetical ‘person of ordinary skill in the art’ when the invention was unknown and just before it was made.” In view of the available factual information, the examiner must make a determination as to whether the claimed invention “as a whole” would have been obvious at that time to a person of ordinary skill in the art. Importantly, a rejection based on these criteria must be based on what is taught in the prior art, not the applicant’s disclosure. The applicant’s disclosure may not be used as a blueprint from which to construct an obviousness rejection.

Exemplary claim 1 recites a method for providing access to a secure entity or service by M designated persons having only limited access privileges, comprising:

storing biometric data in dependence upon a biometric characteristic of each of the M designated persons;

capturing biometric information representative of a biometric characteristic of each of N persons and providing biometric data in dependence thereupon, with  $1 < N < M$  being a subset of a plurality of predetermined subsets of the M designated persons, wherein at least two of the predetermined subsets of the plurality of predetermined subsets of the M designated persons have different access privileges to the secure entity or service;

comparing the captured biometric data of each of the N persons of the subset with the stored biometric data to produce N comparison results; and,

if the N comparison results are indicative of the N persons of the subset each being one of the M designated persons and thereby forming the subset of the N persons, determining the access privileges to the secure entity or service in dependence upon the subset of the N persons.

Applicant submits that the Examiner has not provided a suggestion or motivation to enable one skilled in the art to combine the teachings of the references as proposed by the Examiner and, in any case, the proposed combination of teachings does not teach or suggest all of the claim limitations in the independent claims. In view of the fact that any combination of Matyas, Jr. et al., Schneier, and the admitted prior art taken together do not teach all of the claimed features of the independent claims, even if the teachings of these references could be combined as the Examiner suggests, the method and system of independent claims 1, 7, 10, and 14 would not result. The Examiner has thus failed to establish *prima facie* obviousness and the rejection of claims 1, 2, 4, 5, and 7-18.

As noted in the previous amendment response, Matyas, Jr. et al. disclose a biometric based multi-party authentication system in which a plurality of valid biometric authentication messages are accumulated for a corresponding plurality of users and, if an authentication threshold value is exceeded, an indication of authentication is provided. For example, once  $k$  users out of  $n$  users are authenticated, where  $0 < k < n$ , then authentication is provided. In an alternative embodiment, a secret value is distributed across multiple users by dividing the secret value into a plurality of shares. The secret value is recovered by obtaining a sampled canonical biometric template from  $k$  users, where  $0 < k < n$ . As acknowledged by the Examiner, Matyas, Jr. et al. provides no teaching of providing “a plurality of predetermined subsets of the  $M$  designated persons, wherein at least two of the predetermined subsets of the plurality of predetermined subsets of  $M$  designated persons have different access privileges to the secure entity or service.” For such a teaching, the Examiner now refers to Schneier. However, contrary to the Examiner’s assertions, Schneier also fails to teach a plurality of subsets having different access privileges as claimed.

Schneier teaches at page 71, third paragraph of section 3.7, that one user (a general) may have more keys than other users (colonels) in order to provide authentication. In the example given, the general has 3 keys while the colonels have one each, where 5 keys are required for authentication. In the context of the Matyas, Jr. et al. system, this teaching would suggest that authentication of one user could provide a greater authentication value (quantity) towards the authentication threshold value than authentication of other users. However, this teaching, if combinable with Schneier, would not suggest that respective subsets of users have different access privileges. Once the authentication threshold value is

reached, neither Matyas, Jr. et al. nor Schneier suggest that the users have anything but equal and full access privileges.

Similarly, Schneier teaches at page 72, first paragraph, that different users (e.g. users on different floors) may contribute more or less to the authentication threshold value. In the context of the Matyas, Jr. et al. system, this teaching would once again suggest that authentication of one user could provide a greater authentication value (quantity) towards the authentication threshold value than authentication of other users. Once again, this teaching, if combinable with Schneier, would not suggest that respective subsets of users have different access privileges. Once the authentication threshold value is reached, neither Matyas, Jr. et al. nor Schneier suggest that the users have anything but equal and full access privileges.

Finally, Schneier teaches at page 73, under the section heading “Secret-Sharing Schemes with Prevention,” that a secret may be divided a first number of ways (10) to reconstruct the secret and that the secret may be divided a second number of ways (20) to prevent others from reconstructing the secret. In the context of the Matyas, Jr. et al. system, this teaching would suggest that authenticated users could vote to add or subtract from the authentication threshold value. Yet again, this teaching, if combinable with Schneier, would not suggest that respective subsets of users have different access privileges. Once the authentication threshold value is reached, neither Matyas, Jr. et al. nor Schneier suggest that the users have anything but equal and full access privileges.

One skilled in the art would thus appreciate that Schneier does not teach providing different access privileges to different subsets of users in the manner claimed. As noted in the specification, different access privileges to services by different subsets of users means that the different subsets of users, once authenticated, are only able to access portions or all of the secure entity or service as set by the person or entity establishing the privileges. In the example given in the specification, one subset of users, once all are authenticated, may access a bank vault, while a different subset of users, once all are authenticated, may access the gold bars in the bank vault. Neither Matyas, Jr. et al. nor Schneier provide teachings whereby biometric data of N persons out of M persons,  $N < M$ , may be captured and authenticated to provide such different access privileges to a secure entity or service as claimed. In the absence of such teachings, Matyas, Jr. et al. taken separately or together do not teach or suggest all of the claim limitations and hence cannot establish a *prima facie* case of

obviousness, even if the teachings of these references are combinable as proposed by the Examiner. To the extent the Examiner suggests to the contrary in the Final Rejection, Applicant respectfully disagrees. Withdrawal of the rejection of claims 1, 2, 4, and 5 as being obvious over the teachings of Matyas, Jr. et al. and Schneier is respectfully solicited.

The “admitted prior art” referenced in paragraph [0012] of the specification is cited with respect to claims 7-17 for reference to a portable fingerprint recognition and transmission device. Such teachings are irrelevant to the shortcomings in the teachings of Schneier noted above with respect to claim 1. Accordingly, even if one skilled in the art would have modified the system of Matyas, Jr. et al. to implement the secret sharing techniques taught by Schneier in a portable fingerprint recognition transmission device of the type described in paragraph [0012] of the specification, the claimed method and system would not result. Each of independent claims 7, 10 and 14 have been previously amended to reference the capture of biometric data of N persons out of M persons, N<M, and authentication of same to provide different access privileges to a secure entity or service. Inasmuch as such features are not taught by Matyas, Jr. et al., Schneier, or the admitted prior art, the Examiner has not established *prima facie* obviousness with respect to claims 7-17 either. Withdrawal of the rejection of claims 7-17 as being obvious over the teachings of Matyas, Jr. et al., Schneier, and the admitted prior art is respectfully solicited.

Finally, Schneider et al. is cited with respect to claim 18 for allegedly teaching the use of a smart card as a handheld portable biometric device. Such teachings are irrelevant to the shortcomings in the teachings of Schneier noted above with respect to independent claim 14 from which claim 18 depends. Accordingly, even if one skilled in the art would have modified the system of Matyas, Jr. et al. to implement the secret sharing techniques taught by Schneier in a portable fingerprint recognition transmission device of the type described in paragraph [0012] of the specification, where the device was implemented on a smart card as purportedly taught by Schneider et al., the claimed invention still would not result. Inasmuch as such features are not taught by Matyas, Jr. et al., Schneier, the admitted prior art, or Schneider et al., the Examiner also has not established *prima facie* obviousness with respect to claim 18. Withdrawal of the rejection of claim 18 as being obvious over the teachings of Matyas, Jr. et al., Schneier, the admitted prior art, and Schneider et al. is respectfully solicited.

DOCKET NO.: IVPH-0067/12-61 US  
Application No.: 09/940,795  
Office Action Dated: August 9, 2005

PATENT  
REPLY FILED UNDER EXPEDITED  
PROCEDURE PURSUANT TO  
37 CFR § 1.116

The Examiner has further failed to provide a *prima facie* case of obviousness with respect to any claim since the Examiner has not met his burden of providing a suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to combine the reference teachings. Instead, the Examiner has provided general references to increasing the "versatility of the system," taking advantage of the "smaller, lighter, less burdensome, and more portable miniaturized devices," or minimizing "delay and inconvenience." Applicant submits that such general statements of motivation to combine made by the Examiner, without support in the references themselves or evidence that suggestions to combine are in the knowledge generally available to one skilled in the art, do not meet the Examiner's initial burden of factually supporting any *prima facie* conclusion of obviousness. Such a piecing together of disparate teachings, without sufficient motivations or suggestions to combine, suggest to Applicant that the Examiner has used Applicant's disclosure as a blueprint for the obviousness rejections. Accordingly, if the Examiner elects to maintain one or more of the obviousness rejections, the Examiner is strongly urged to clearly articulate the evidence of suggestions, motivations, or knowledge possessed by those skilled in the art that would have led one skilled in the art to combine several prior art teachings to arrive at the claimed invention.

For the above reasons, withdrawal of the obviousness rejection of all claims and withdrawal of the finality of the official action are respectfully requested.

**Conclusion:**

Entry of the above amendments in view of the above remarks is believed to overcome all rejections and to place the present application in condition for allowance. A Notice of Allowability is respectfully solicited.

Date: February 9, 2006



Michael P. Dunnam  
Registration No. 32,611

Woodcock Washburn LLP  
One Liberty Place - 46th Floor  
Philadelphia PA 19103  
Telephone: (215) 568-3100  
Facsimile: (215) 568-3439